April 21, 2020

To:
Paul DeVillers
Chief Electoral Officer
Métis Nation of Ontario

Re:
Summary of Security Protocols for Electronic & Phone Voting

Dear Mr. Paul DeVillers, MNO Chief Electoral Officer

I am pleased to share with you a summary of our security protocols for electronic and phone voting. OneFeather is cloud based software designed with the most current and leading cyber security technologies and data protection architecture available. All of our software also utilizes the latest encrypted technologies in all transmissions and storage, and moreover we utilize Canadian AWS servers (including multiple firewalls) – ensuring the best data protection measures available.

Voters wishing to access either electronic or telephone voting may only do so following activation of their OneFeather profile which utilizes a number of steps to authenticate and verify a voter's identity. Once this step is completed, which includes a traditional 2-step verification process - the eligible voter is then also provided a PIN (personal identification number) unique to the voter and the voting event. If the voter does not have an email and wish to vote by phone, we provide their PIN directly to the voter following a verification process over the phone.

In order to vote successfully the eligible voter must utilize the secure voting link to ballot we provide or the toll-free number, along with their Citizenship No, Date of Birth and the PIN. If anyone of these critical pieces is absent or otherwise used incorrectly – the voter will not be permitted to Vote, and the Chief Electoral Officer will be notified of any flagged members experience voting difficulties.

Other security features limit the use of only one (1) email to be used per voter – emails can not be shared or used by more than one eligible voter. We also have a number of security features which monitor 24/7/365 IP use (your computer or smart device), and brute force attacks or other attempts by bad actors to compromise the voting event. Finally, our systems track each vote, all voter activity and each voting attempt in an immutable ledger for audit and appeal purposes if needed.

OneFeather is also designed to ensure that each eligible voter is only able to vote only once for the prescribed ballots for which they are entitled to vote. We accomplish this through some sophisticated and innovative software development which essentially pairs 'tags' between ballots and voter data – effectively revealing only the ballots available to that voter and making ineligible ballots inaccessible.

While no online or digital solutions can guarantee 100% impenetrability to bad actors and unscrupulous types, we are very proud of our track record and continue to invest in the best security features and protocols available to ensure your successful voting event.

Sincerely,

Lawrence Lewis, Founder

OneFeather

OneFeather